soBGP

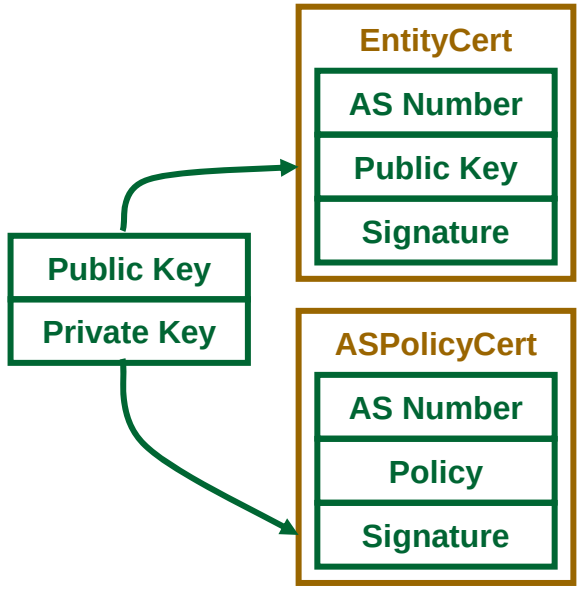
SIDR BOF/IETF Vancouver

Russ White/riw@cisco.com

soBGP Goals

- Do not touch existing BGP packets
  - *Do not touch existing BGP implementation optimizations*
- Allow partial deployments*Not all AS' need to deploy to be useful*
  - *Not all pieces of soBGP need to be deployed to be useful*
- Deploy with existing hardware
- Distribute information
  - *No centralized servers!*
- Provide security information
  - *Local AS controls security policy (within bounds)*

Certificates



- EntityCert
  - Ties AS number to public key(s)
  - Signed by some trusted third party
    - Web of Trust??
    - Centralized Authority??
    - *Depends on the deployment!*
- ASPolicyCert
  - Contains AS level policy
  - Contains list of transit peering AS'
    - Does not contain information about number, or level, or peering arrangements, etc.
    - Level/type of policy exposure is completely AS determined
  - Multiple ASPolicyCerts, with different policies advertised to each peer, are *possible*
  - Signed by advertising AS, using private key pair of public key advertised in EntityCert

Certificates

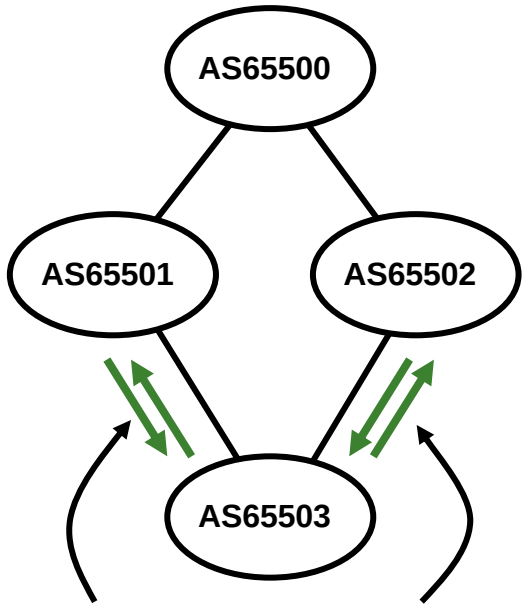
- AuthCert
  - Ties an originating AS to an address block
  - Signed by trusted third party
    - For instance, could be signed using registry provided certificate tying a fully qualified name to an address block
    - No need for an AS at address owner—the address owner can authorize the originating AS to originate specific prefixes within the address block
- PrefixPolicyCert
  - Contains the Authcert + per prefix policy, if any exists
  - Policy is added when needed, (hopefully) limiting the extent of per prefix policy carried through the system
  - An origin AS *can* advertise different policies to different peers, etc.

Certificate Transport

- There is a transport draft
  - New BGP message type
    - Doesn't touch existing BGP packets
  - Capabilities define if certificates are exchanged
    - Certificates only
    - NLRIs only
    - Certificates and NLRIs
    - Certificates with the assumption that they are already cryptographically checked *(iBGP only)*
  - Allows a wide range of deployment options
  - But….
    - *Any mechanism to distribute certificates is fine*
    - *BGP peering semantics are conveniently already defined….*

Validation of Routing Information

- Build a graph of transit AS interconnectivity
  - Based on the transit peerings exposed in ASPolicyCerts
  - Policy can be “hung off of” this graph *if desired* and *exposed*
  - A link must be advertised in both directions to be considered valid



AS65503 advertises a connection to AS5501; AS 65501 advertises a connection to AS65503; the link is valid

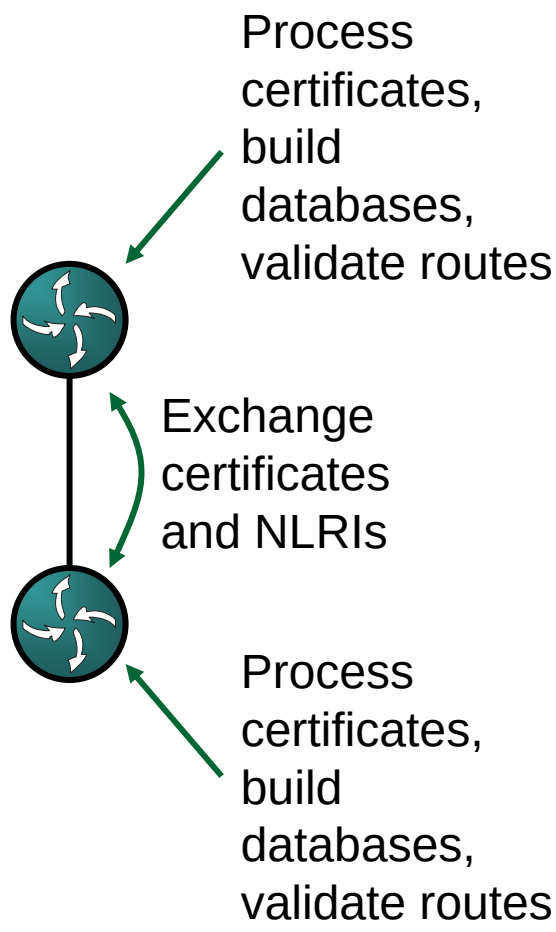
AS65503 advertises a connection to AS5501; AS 65501 advertises a connection to AS65503; the link is valid

Validation of Routing Information

- Check origin AS against received AuthCerts
  - Discard if no authorized originating AS
- Check first hop AS in AS Path
  - Against list of AS' advertised as peering by originating AS
  - Adjust security preference as needed
- Check AS Path against graph
  - Adjust security preference as needed
- Check policies against graph and prefix policies
  - Adjust security preference as needed
- Check security preference against local policies

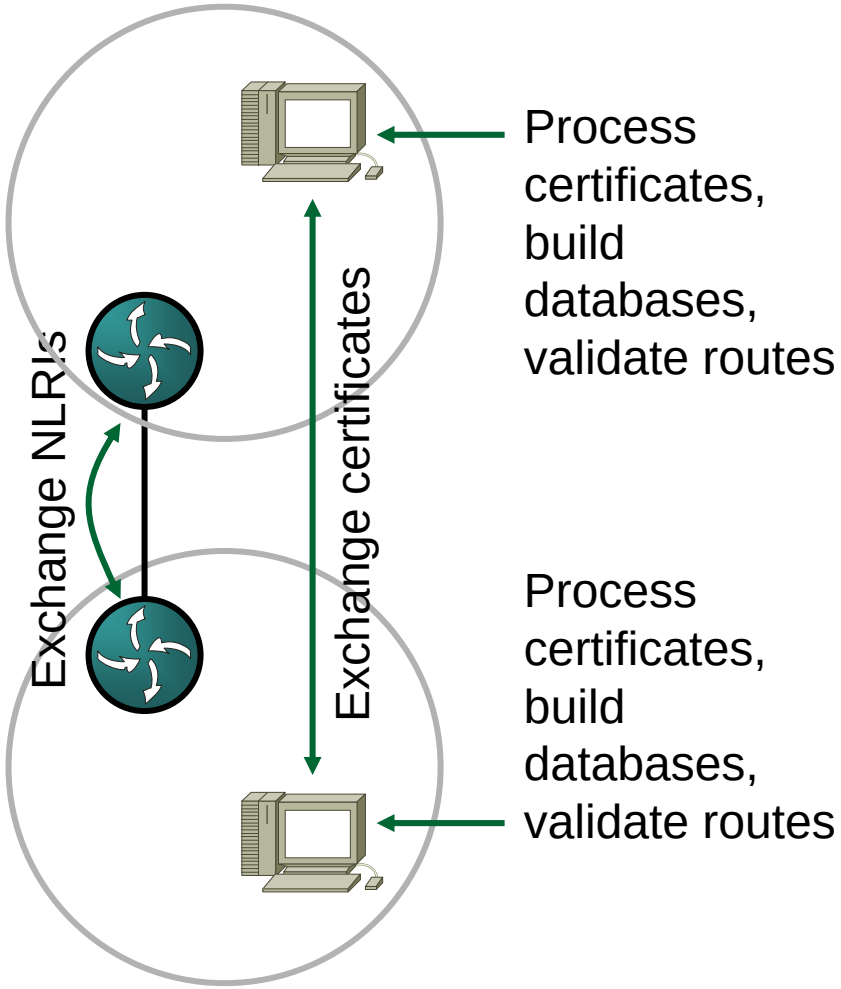
Deployment Option 1

- eBGP speakers exchange:
  - NLRIs
  - soBGP certificates
- Each edge router:
  - Processes all received certificates locally
  - Build databases
  - Make policy decisions based on local configuration
- We can limit processing somewhat by allowing certificates learned through iBGP sessions to be trusted
- *This is the "improve Cisco's stock price" option!* ☺



Deployment Option 2

- soBGP speakers:
  - Exchange certificates
  - Process certificates, build databases, etc.
- eBGP speakers:
  - Exchange NLRIs
  - Use “protocol X” to gather security preferences for received routes
  - Modify routes based on local security policies combined with security preference returned from soBGP server
- *A large number of variant options between these two are also possible*

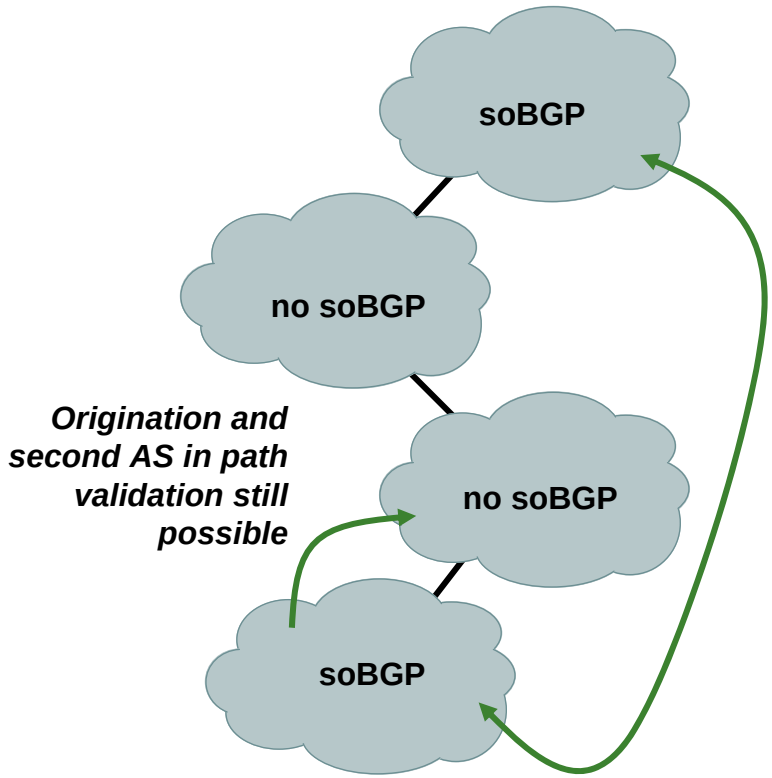


Partial Deployments

- There are two axis along which soBGP may be partially deployed
  - In physical space; not all AS' run soBGP
  - In logical space; not all checks are "turned on"

Physical Space Partial Deployment

- Multihop sessions, or other techniques (including possible HTML access) are used to transport certificates between AS' running soBGP
- Route validation remains the same except….
  - You only check the AS interconnections for intervening AS' which are advertising ASPolicyCerts
  - Local policy dictates how to handle more and less completely checked paths



Logical Space Partial Deployment

- Simply don't use the AS Path graph or policy checks
  - *But, we believe these checks are important!*
- The Internet could "grow into" these checks over time
- *Logical and physical space partial deployments are possible at the same time, of course….*

soBGP

- Drafts: search on draft-*-sobgp in the repository
- ftp://ftp-eng/sobgp/index.html
- Questions, thoughts, suggestions, etc., all welcome